BraxSecure

HIPAA Compliant Message Portal

BraxSecure User Manual

Quick Start Guide

1. Mobile Phone – Go to URL https://www.braxsecure.com/mobile and add shown Mobile App to Home Screen.

2. Enter your Login Information on the Login/Logout Section and tap Save Login.

3. Desktop Computer – Go to URL:
   https://www.braxsecure.com/prod/loginstaff.php
   Then bookmark the page and add to the Bookmark Bar.

4. Enter your Login Information and select Message Manager.

5. Start Filling in your Address Book and determine what you will use as your Challenge Message and Verification Key for each of your recipients.

6. Add Additional Login ID's for Staff Members who will be using the App (if allowed in your subscription).

You are ready to send messages!

We Care About Your Security

Congratulations on your decision to subscribe to BraxSecure. You must know now that when you've been doing things on the internet like as emailing, using mail providers like Gmail, Yahoo, MSN, Texting, messaging on Facebook , that everything you do is visible to anyone with a simple software tool called a Sniffer or your messages and information is visible to the employees of those services. If you didn't know specifically how it is done, now, you will have learned that everything mentioned above is readable in plain text. This is why HIPAA laws specifically prohibit sending Medical information view the above means.

Now you are protected. We will explain how.

BraxSecure examines all the aspects of handling your messages in a secure way at all levels. The web servers require use of SSL (https appears in the URL) so that your interactions with the web server are not visible to anyone else. SSL stands for Secure Sockets Layer. So when you send your message, you are secure in the knowledge that your message was not intercepted in any way on its way to the BraxSecure database.

Once the message is saved in the database, the message itself is encrypted with a technology called SHA-1 512 bit. This is one of the top level encryption algorithms in use today. Because of this, even a person reading the information in our database cannot read the message or decipher it. Only the receiver and the sender can see it. So no casual viewer of a BraxSecure server can help anyone to read the message.

The staff at BraxSecure are trained to protect your interests at all times and maintain the best security practices at the server side to prevent data compromise. We have implemented policies, including message lifespans, to lessen the chances of a security breach.

At the receiving end, a recipient is passed a message through a link to the SSL secured portal. A hacker with sniffing software on the internet will never see the actual message being transmitted. The text message does not reveal the recipient and the email has very limited information, simply stating that a Secure Message has been sent.

If a hacker attempts to break the Verification Key of a message, the Key will automatically be changed, thus creating a situation of unlimited possibilities for a password.

It is up to you to establish additional layers of security as your application demands. For example, you can have randomly assigned verification keys. For ease of use, you can keep the Verification Keys simple and easy to remember. All this is your choice since the security level depends on the likelihood of a security attack. It will depend on the balance between ease of use and security.

For HIPAA privacy laws, simply using the system even with the simplest Verification key will satisfy the law since one cannot randomly see the messages.

For your own protection, use complex passwords (combining numbers and letters and at least 8 characters in length). Limit the staff members who can have access to the Messages and limit who of them have Administrator rights.

The system tracks all activity of each Login ID. For this reason, it is important that users do not share Login ID’s.

On a mobile device, we are more lenient because accuracy of data entry is more important. Login Information will be retained on the Mobile device until you specifically log out. If your account is compromised through the theft or loss of your Mobile device, immediately go to the Desktop version of the app and change your password.

When changing phones, make sure to specifically Log Out from the App. This will remove the password from the phone. Phones have an option to delete the data associated with the different Apps. If you perform this deletion, all private information on the phone will be removed.

It is OK to allow cookies on the Phone or Desktop. We don’t keep your passwords in cookies on the Desktop App, and cookies are not used in the Mobile App. We also turn off autocomplete features in the browser to prevent your login information from being saved outside of the app.

As it will be explained later, messages are viewed by all staff members using a shared Message Master Key. This allows everyone to keep knowledge of their individual login passwords to themselves. Each user can also change their password at any time and it is conveniently accessible.

A. Installation

1. You will have been provided with an initial set of user identification credentials to log into BraxSecure.

   Subscriber ID: _________________________ (System Assigned Numeric Value)

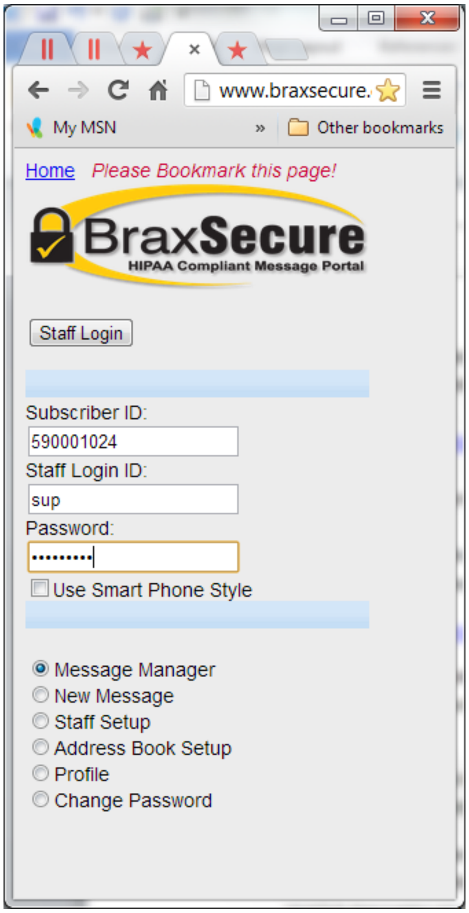
   Login ID: ______________________________ (Admin Login ID)

   Password: _____________________________ (at least 8 characters long)

2. Installation of the Web App on a Desktop Computer is accomplished by going to the URL below on a browser and bookmarking it.

   https://www.braxsecure.com/prod/loginstaff.php

   This will display the login page below.



Subscriber ID: 590001024

Staff Login ID: sup

Password: ••••••••

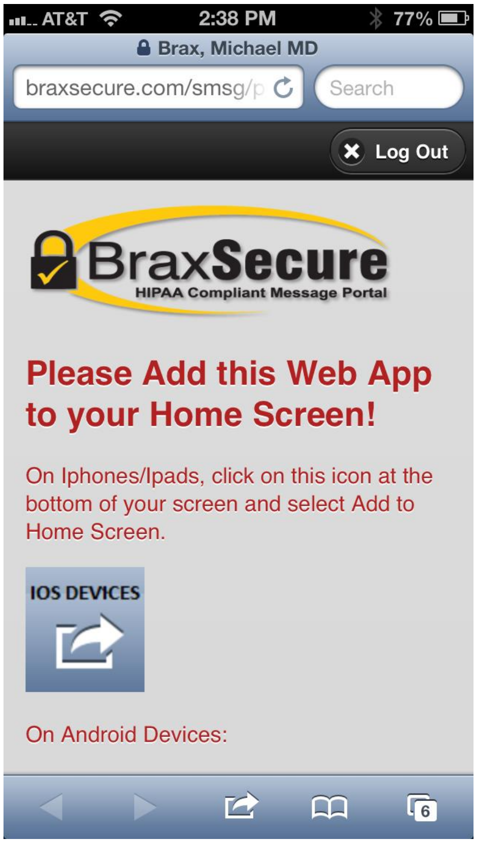
□ Use Smart Phone Style

● Message Manager
○ New Message
○ Staff Setup
○ Address Book Setup
○ Profile
○ Change Password

Use the credentials provided above to log in.

3. There is also a Mobile App version for your Smart Phone (Iphone, Android, Windows Phone, Blackberry). Using the browser of your phone, go to the URL below.

   https://www.braxsecure.com/mobile

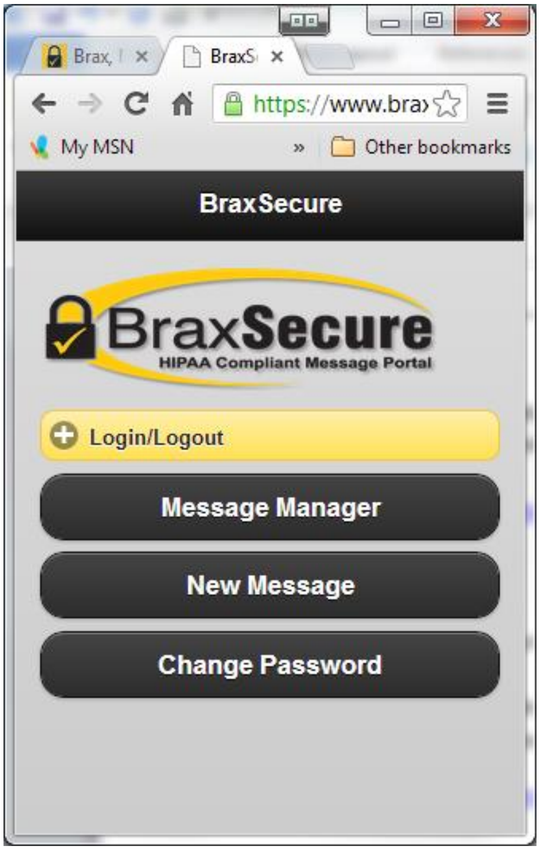


Please Add this Web App to your Home Screen!

On Iphones/Ipads, click on this icon at the bottom of your screen and select Add to Home Screen.

On Android Devices:

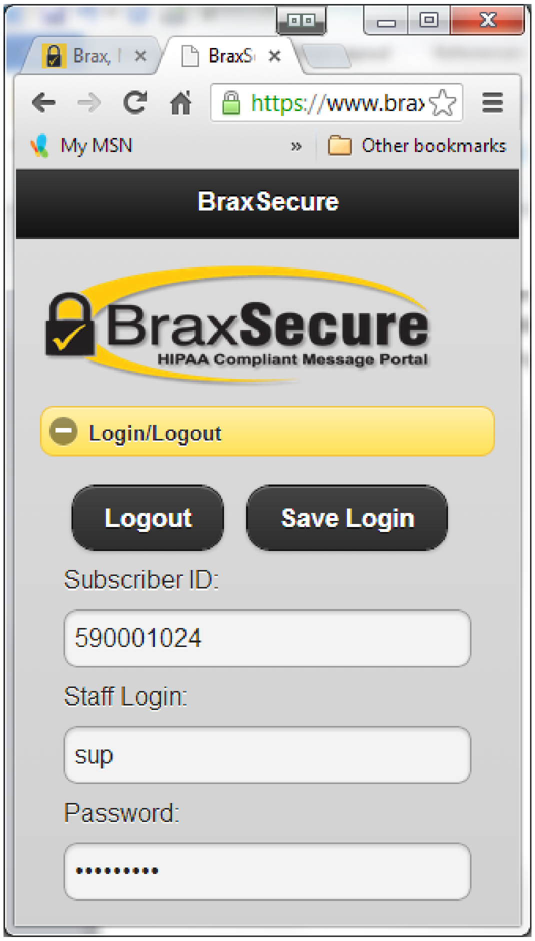
You will be asked to add the App to the Home Screen before using it. After the App is added to the home screen, it will behave just like a native App on the phone downloaded from an App Store (like Itunes). Once you start the app from the Home Screen, it will appear as shown on the image below.



4. If you have not used it before, only the Login/Logout button will be visible on the page.

5. To start using the App, login using the credentials provided. On a Desktop computer, if Cookies are enabled (you should enable them) in your browser, the system will remember the Subscriber ID and only the Staff Login ID and Password need to be provided.
   On a Smartphone, expand the Login/Logout are by tapping on the yellow bar and the Login window will be displayed below. Save your login and it will remember the information for the future. You will not need to reenter the Login Information unless you delete the App or tap on the Logout button.

   If you install multiple instances of the App on the Home Screen, please note that each App will operate independently and not share login data with another App on the same phone



Subscriber ID:

590001024

Staff Login:

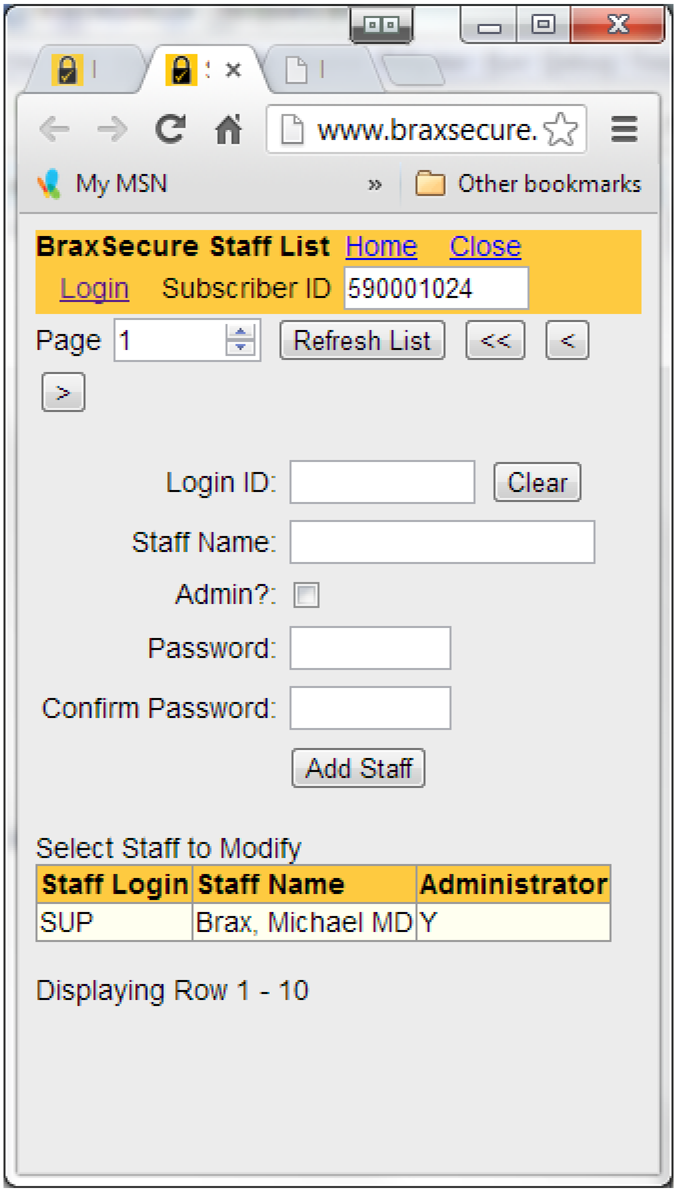
sup

Password:

•••••••••

6. The first thing to do on the Desktop Computer side is to set up additional Login ID's for the staff members of the Subscriber ID which is a single Text/Email Recipient account.

   From the Login Page of the Desktop Web App, click on Staff Setup after entering credentials for an Admin account and Login.



BraxSecure Staff List Home Close

Login Subscriber ID 590001024

Page 1 Refresh List << <

>

Login ID: Clear

Staff Name:

Admin?: □

Password:

Confirm Password:

Add Staff

Select Staff to Modify

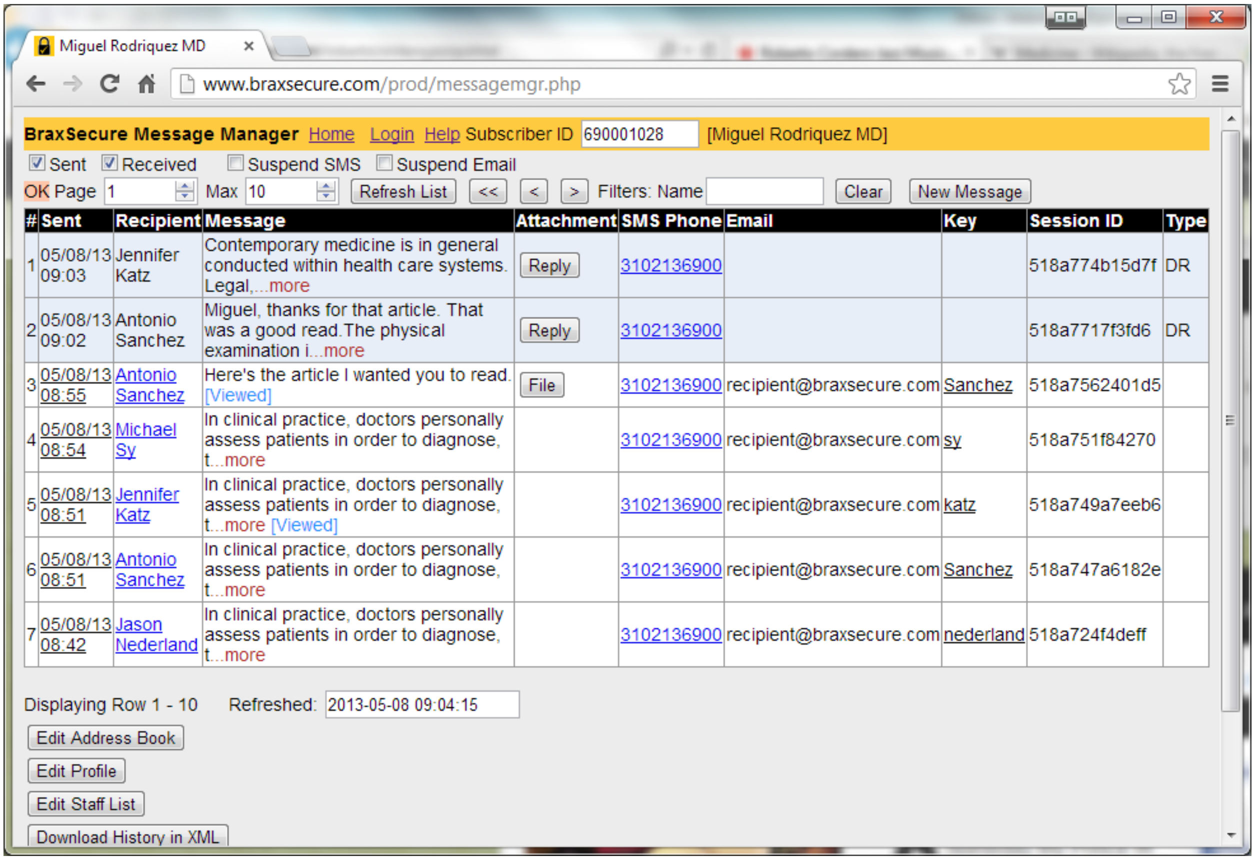
Staff Login	Staff Name	Administrator
SUP	Brax, Michael MD	Y

Displaying Row 1 - 10

Using the page displayed above, you can start adding Login ID’s. Each Login ID has to be unique, and grant Admin accounts sparingly, since it enables that user to Add and Delete other users. Once Login ID’s are established, all the users may use the App completely for sending receiving messages, with Admin privileges to change the Staff List, and Account Profile limited to some users.

A. Message Manager

The next thing to determine is how you intend to send and receive messages. You can use the Desktop App by itself if you wish to control the entire message flow from here.



BraxSecure Message Manager Home Login Help Subscriber ID 690001028 [Miguel Rodriquez MD]

☑ Sent ☑ Received □ Suspend SMS □ Suspend Email

OK Page 1 Max 10 Refresh List << < > Filters: Name Clear New Message

#	Sent	Recipient	Message	Attachment	SMS Phone	Email	Key	Session ID	Type
1	05/08/13 09:03	Jennifer Katz	Contemporary medicine is in general conducted within health care systems. Legal,...more	Reply	3102136900			518a774b15d7f	DR
2	05/08/13 09:02	Antonio Sanchez	Miguel, thanks for that article. That was a good read.The physical examination i...more	Reply	3102136900			518a7717f3fd6	DR
3	05/08/13 08:55	Antonio Sanchez	Here's the article I wanted you to read. [Viewed]	File	3102136900	recipient@braxsecure.com	Sanchez	518a7562401d5	
4	05/08/13 08:54	Michael Sy	In clinical practice, doctors personally assess patients in order to diagnose, t...more		3102136900	recipient@braxsecure.com	sy	518a751f84270	
5	05/08/13 08:51	Jennifer Katz	In clinical practice, doctors personally assess patients in order to diagnose, t...more [Viewed]		3102136900	recipient@braxsecure.com	katz	518a749a7eeb6	
6	05/08/13 08:51	Antonio Sanchez	In clinical practice, doctors personally assess patients in order to diagnose, t...more		3102136900	recipient@braxsecure.com	Sanchez	518a747a6182e	
7	05/08/13 08:42	Jason Nederland	In clinical practice, doctors personally assess patients in order to diagnose, t...more		3102136900	recipient@braxsecure.com	nederland	518a724f4deff	

Displaying Row 1 - 10 Refreshed: 2013-05-08 09:04:15

In the Message Manager window, shown above, you can enable/disable receiving emails and texts using the Suspend SMS and Suspend Email buttons. This will make the Message Manager console the primary user interface for dealing with messages. You can still read and send messages from the Smartphone Apps but you will not get a Text message, thus there will be no ongoing alerts all day.

The best approach is to Suspend Email and SMS (see Checkboxes for this purpose) during the day when there is staff monitoring the account, and then allow the messages to Text to the Physician during off hours as desired. Remember, there is only ONE designated SMS phone and ONE email address.

When viewing the Message Manager, a Status Message appears on the Left side of Page (peach color). This says “Refresh Needed - New Messages” (with a count) if new messages have been sent and warns you to hit refresh to see it. This gets updated every 10 seconds. So a quick glance at that Status Message will tell you if there' s anything new.

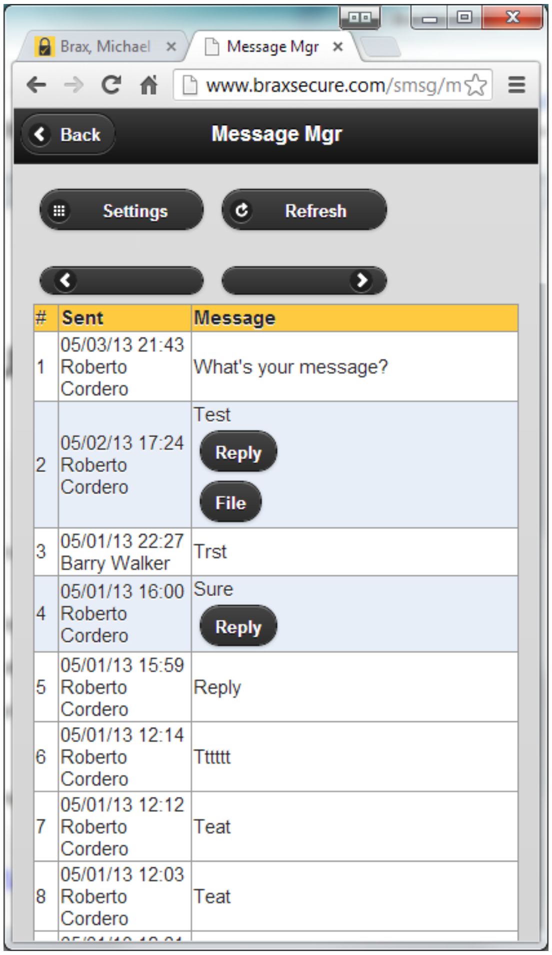
Messages are displayed in the list only partially. If the message is long, you will see "More" at the end of it. Clicking on the message will show the message in its entirety. Also, if a message has been viewed by the recipient, it will end with the word "[Viewed]". This will alert you quickly if perhaps the message was misdirected, or if a resend is required.

You can page through unlimited pages of the messages (ordered from newest first) and you can filter the messages by recipient name.

From the Message Manager console view, a user can control all aspects of message flow. In the above view, the following actions are available:

a. Clicking on the Sent Column of a Message will allow the Message to be resent.
b. Clicking on the Recipient Column of a Message will allow the Message to be opened as it will be received by the Recipient.
c. Clicking the Phone Number on a Mobile Phone will allow you to Dial Out with that number on most Smartphones.
d. Clicking on the Key Column of the Message will allow you to change the Verification Key.

The Mobile App version of Message Manager is simpler and looks like that shown below. Just like the desktop version, the messages themselves can be expanded by tapping on the Message area.

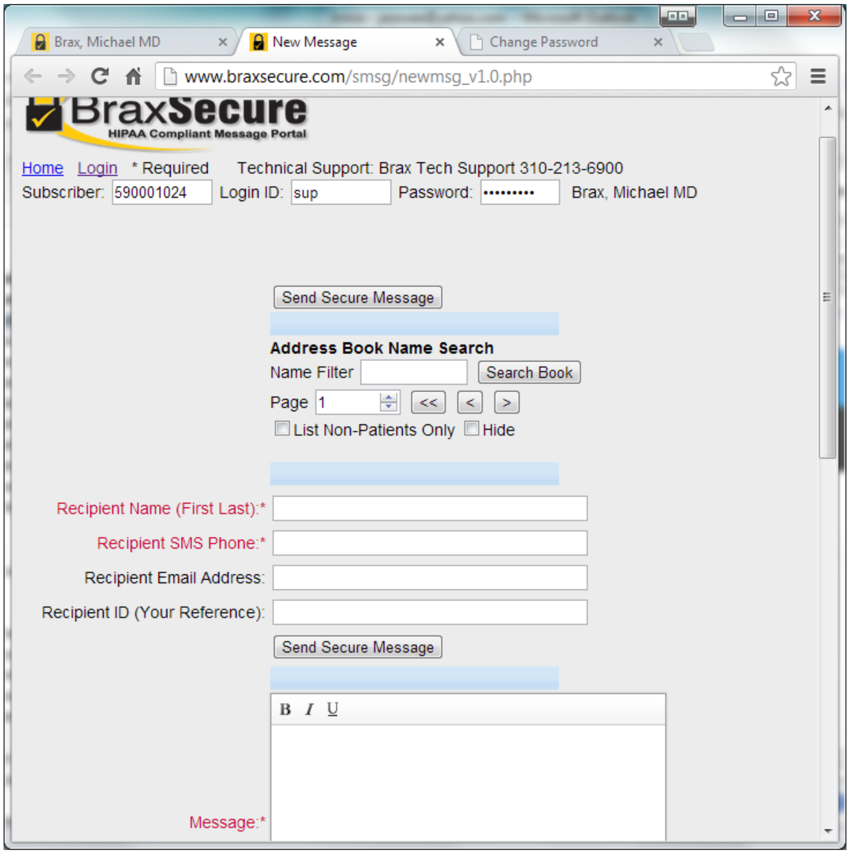


#	Sent	Message
1	05/03/13 21:43 Roberto Cordero	What's your message?
2	05/02/13 17:24 Roberto Cordero	Test Reply File
3	05/01/13 22:27 Barry Walker	Trst
4	05/01/13 16:00 Roberto Cordero	Sure Reply
5	05/01/13 15:59 Roberto Cordero	Reply
6	05/01/13 12:14 Roberto Cordero	Tttttt
7	05/01/13 12:12 Roberto Cordero	Teat
8	05/01/13 12:03 Roberto Cordero	Teat

B. Send Messages

1. Sending a Message is accomplished by clicking on the New Message button in Message Manager, or tapping on Message Manager in the Mobile App. The mobile app version is more simplified. Here are examples of both.

   DESKTOP VERSION



* Required Technical Support: Brax Tech Support 310-213-6900

Subscriber: 590001024 Login ID: sup Password: ••••••••• Brax, Michael MD

Address Book Name Search

Name Filter

Page 1

□ List Non-Patients Only □ Hide

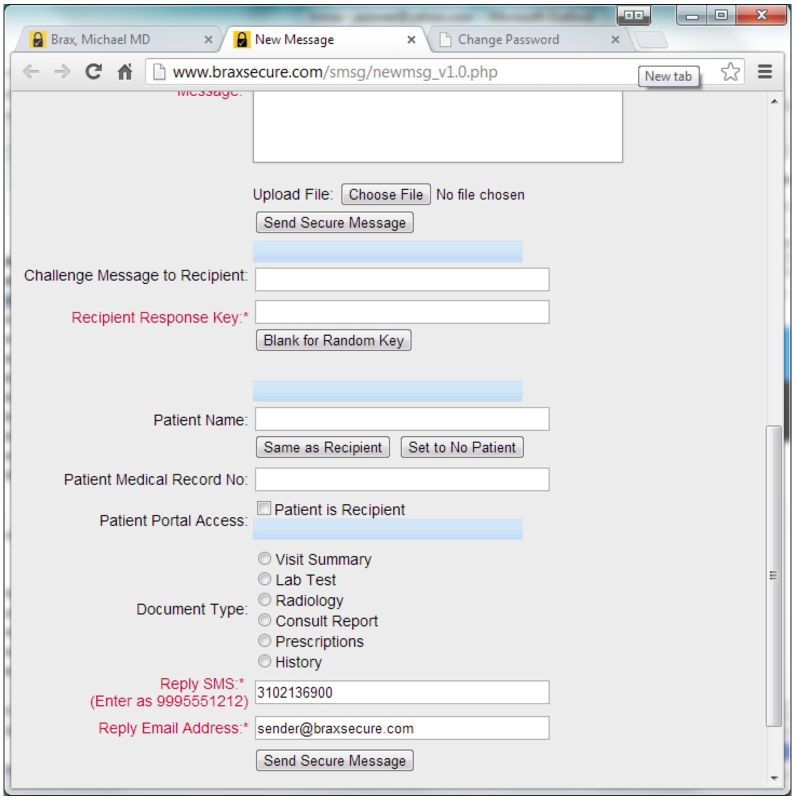
Recipient Name (First Last):*

Recipient SMS Phone:*

Recipient Email Address:

Recipient ID (Your Reference):

Message:*



Message:

Upload File: Choose File No file chosen

Send Secure Message

Challenge Message to Recipient:

Recipient Response Key:*

Blank for Random Key

Patient Name:

Same as Recipient Set to No Patient

Patient Medical Record No:

Patient Portal Access: □ Patient is Recipient

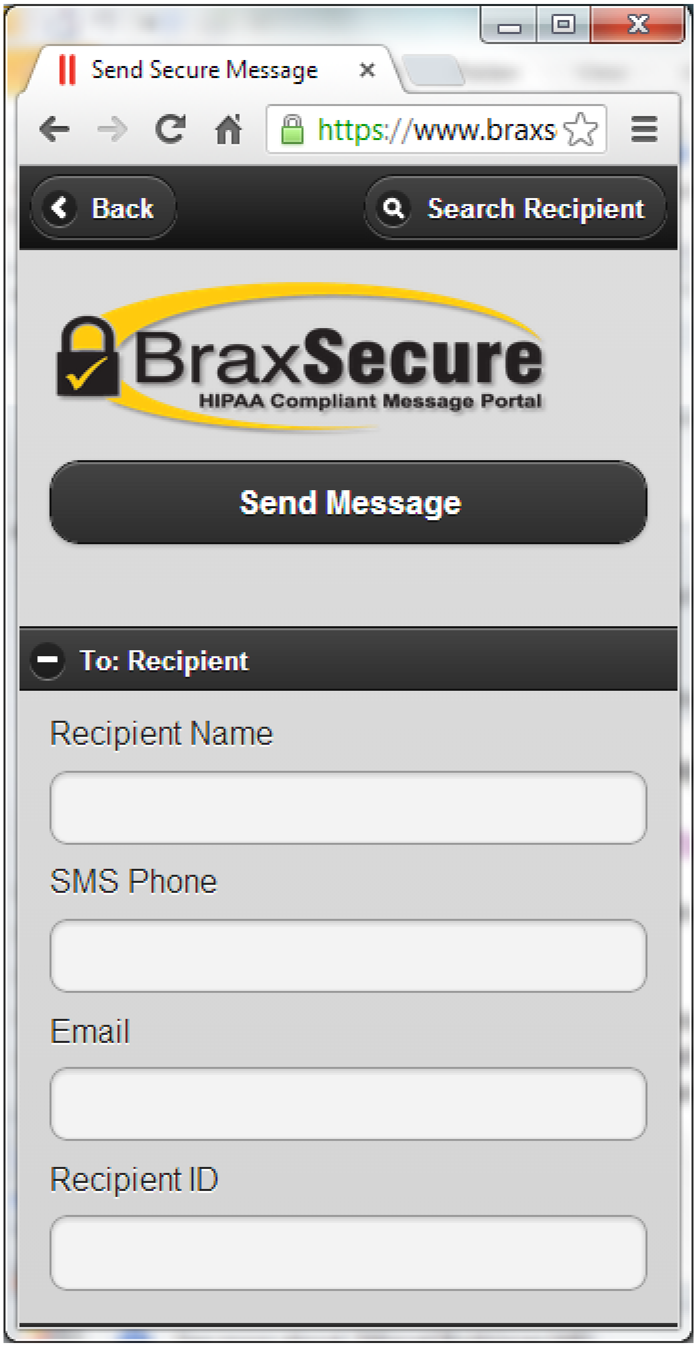
Document Type:
○ Visit Summary
○ Lab Test
○ Radiology
○ Consult Report
○ Prescriptions
○ History

Reply SMS:* (Enter as 9995551212) 3102136900

Reply Email Address:* sender@braxsecure.com

Send Secure Message

MOBILE APP VERSION

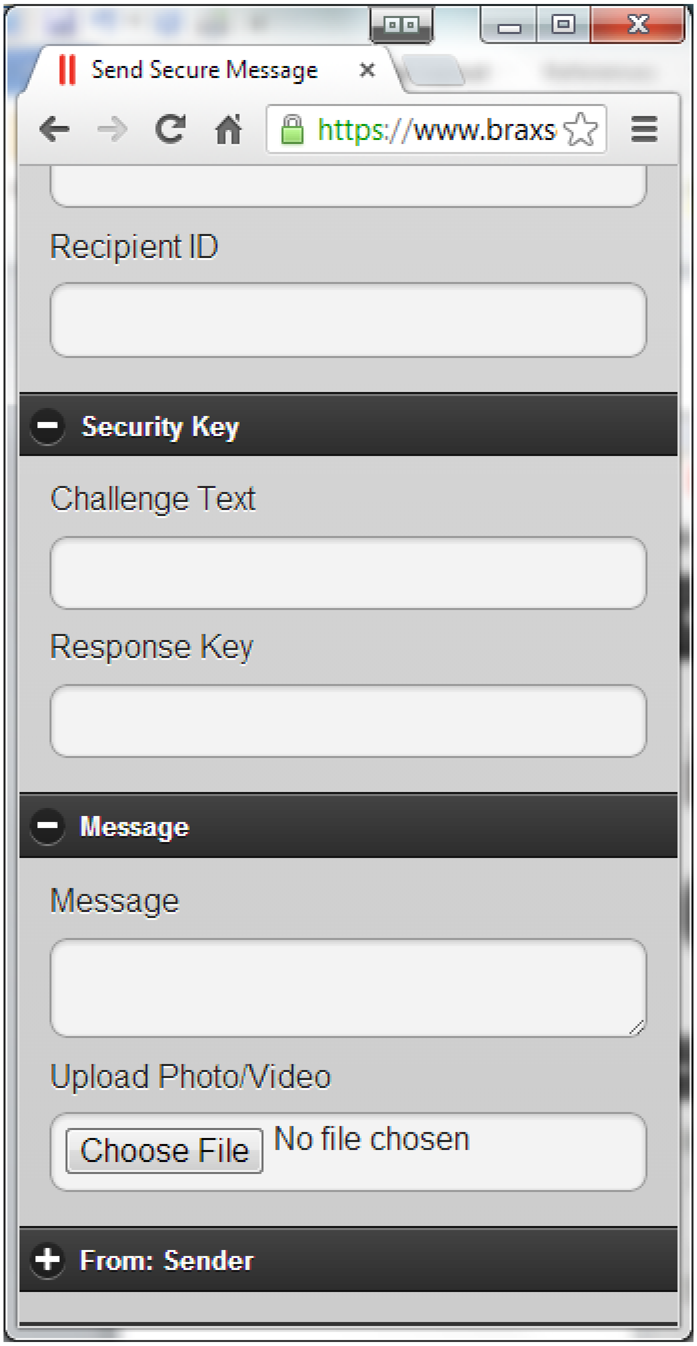


Recipient Name

SMS Phone

Email

Recipient ID



The main difference between the Desktop App and the Mobile App is that, on the Mobile App, you can reference a Patient and specify the document category for the message and any attachments. This is to enable the Patient to look at all the documents in a Patient Portal Application.

2. To send a message, at a minimum you must supply the
    a. Recipient Name
    b. Recipient SMS or Recipient Email (at least one)

c. Challenge Message
d. Challenge Response Key
e. Message Text or a file Attachment
f. Your Sender SMS and Sender Email Address.

The other additional information is useful if you are intending to send messages to a patient for the purposes of adding on a Patient Portal in the future. It is optional.

3. On the Desktop app, you will be able to enter text with formatting. The text entry area allows full HTML formatting so you can actually paste HTML with formatting markup. Or you can use the buttons in the text area to format using Bold, Underline, and Italics.

4. Instead of retyping a Recipient's name, phone and email over and over, all you have to do is Search for Recipients by name using the Search Recipients button. You will be able to select from a list and all the information required, including the preferred Challenge Text/Verification Key will already be preentered. All you have to do is enter the actual message.

   This is why it is very important to try to set up the Address Book in advance as it will save a lot of time later.

   If you are entering a new contact, the recipient information will automatically be saved into the Address Book and will be available for future messages.

C. About the Challenge Response Key

Implementation of BraxSecure needs to be tailored to each application. One of the ways to control the security level of the messages is by the strictness of the Challenge Response Key (or Verification Key as it appears to the Receiver).

One has to understand the different ways a security breach can be accomplished. Without BraxSecure, all messages on the Internet using Text or Email are easily viewed and are completely open to any one with a TCP/IP Sniffer App. This type of breach is now closed. The only thing that an outsider can view is the text message and email message which appears only as:

> Michael Brax MD Secure Message
> http://www.braxsecure.com/prod/vw.php?sid=151434847abca

Since the recipient is not even identified, a simple Challenge Question like "Enter Last Name" would be safe. However, in an email, this question is not a good key because the Last Name is often in the email address. So something known to both the Sender and Recipient is required. It can be a simple thing, like the recipient doctor's office phone number or street name, the doctor's NPI number, the patient's birthdate, the patient's SSNO, to name a few.

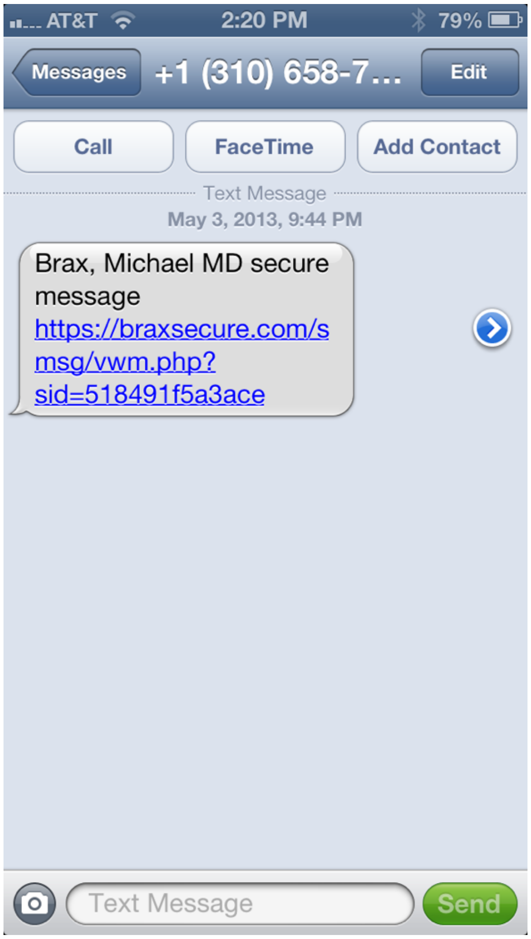
For maximum security, you can leave the Challenge Message and Response BLANK. This will cause the user to receive a prompt to get the Verification Key by separate text. Fortunately, this can be a one-time process since the key will be remembered on the recipient's phone. However, it also requires the extra step and delay of waiting for your verification key.

Note by the way, that in the above scenarios, if an outsider attempts to break in by guessing the key, the system will automatically change the key after 3 failed attempts and a new key will need to be retrieved by text. Since a hacker does not have access to the mobile phone device, there is no way to match messages (the key message to the original message).

In the end, it is up to the sender to determine how secure the messages are. At the very least however, without any serious attempt at hacking, even the most basic security key will pass the HIPAA requirement.

D. Reply and Mobile Message Portal

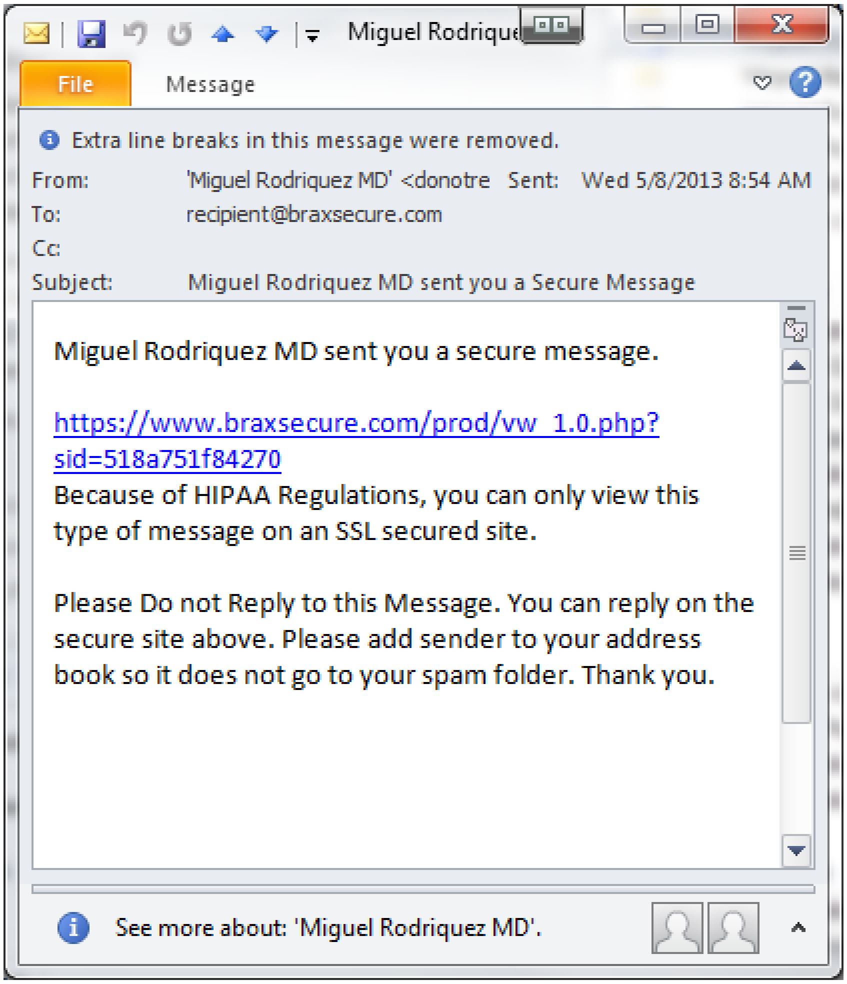
A recipient first receives a text message and email message depending on whether an SMS phone and an email address is supplied. Below is an example message that was received on an Iphone. The message itself that comes before the URL is customizable though still subject to the 144 character limit of a Text Message. The domain is also customizable for a separate charge. Clicking on the link displays the mobile app screen shown on the following image.



May 3, 2013, 9:44 PM

Brax, Michael MD secure message https://braxsecure.com/smsg/vwm.php?sid=518491f5a3ace

The email received by the Recipient will look like the sample below.



Extra line breaks in this message were removed.

From: 'Miguel Rodriquez MD' <donotre Sent: Wed 5/8/2013 8:54 AM
To: recipient@braxsecure.com
Cc:
Subject: Miguel Rodriquez MD sent you a Secure Message

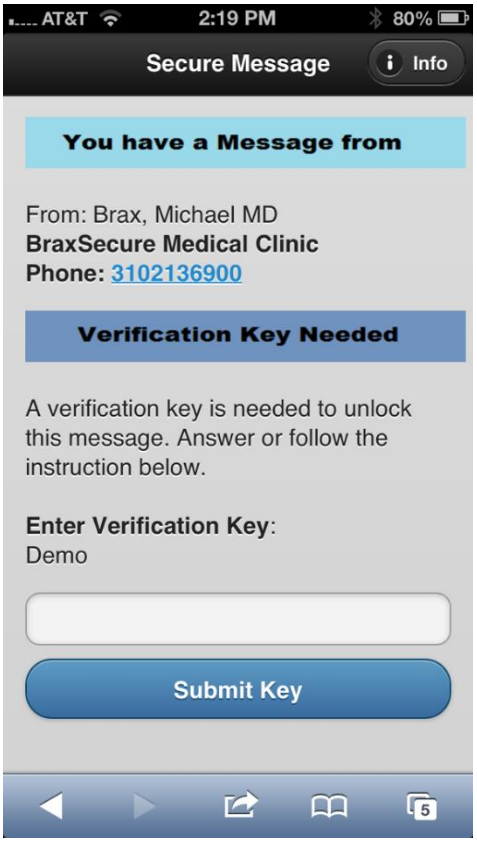
Miguel Rodriquez MD sent you a secure message.

https://www.braxsecure.com/prod/vw_1.0.php?sid=518a751f84270
Because of HIPAA Regulations, you can only view this type of message on an SSL secured site.

Please Do not Reply to this Message. You can reply on the secure site above. Please add sender to your address book so it does not go to your spam folder. Thank you.

See more about: 'Miguel Rodriquez MD'.

The example below shows what is seen by the recipient after clicking on the Text message or email message hyperlink as shown above. Two images are shown because scrolling is necessary to see the whole page.



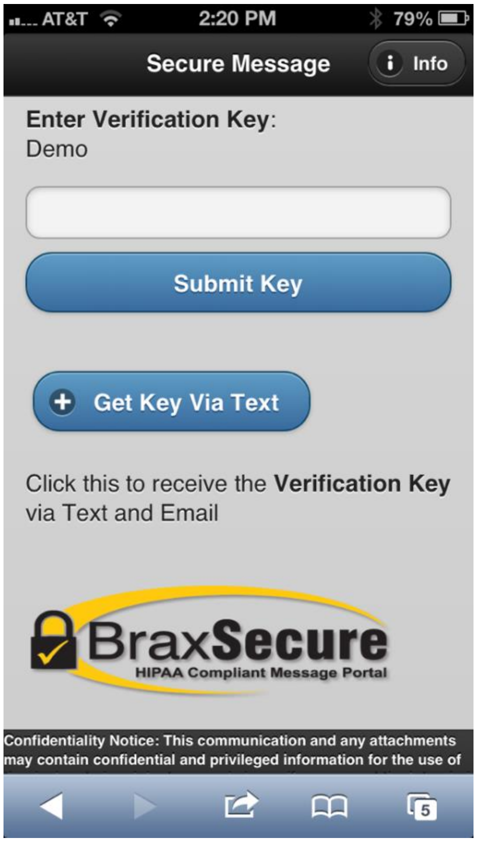
You have a Message from

From: Brax, Michael MD
BraxSecure Medical Clinic
Phone: 3102136900

Verification Key Needed

A verification key is needed to unlock this message. Answer or follow the instruction below.

Enter Verification Key:
Demo



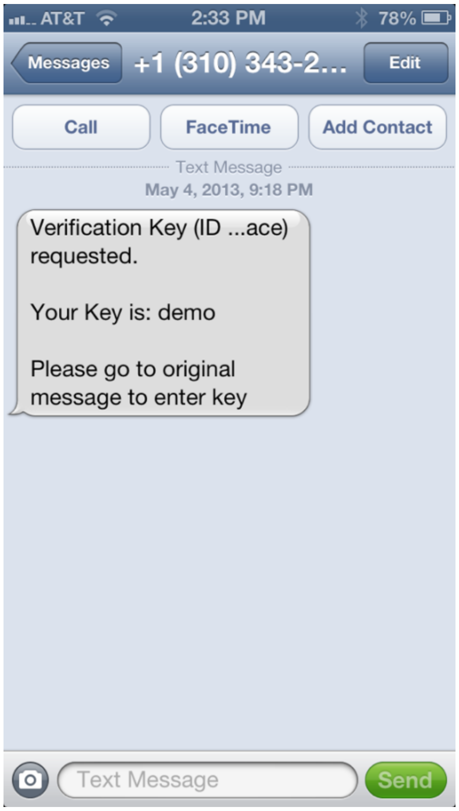
Enter Verification Key:
Demo

Click this to receive the **Verification Key** via Text and Email

Confidentiality Notice: This communication and any attachments may contain confidential and privileged information for the use of

A recipient will be prompted with a challenge question which appears under the prompt "Enter Verification Key". After entering the verification key, the recipient taps on Submit Key. Only 3 attempts are allowed. After that, the system will change the key and it can only be retrieved by Text.

At any time, the user can tap on "Get Key Via Text" to be sent a copy of the key. The Key message will look like that shown below.



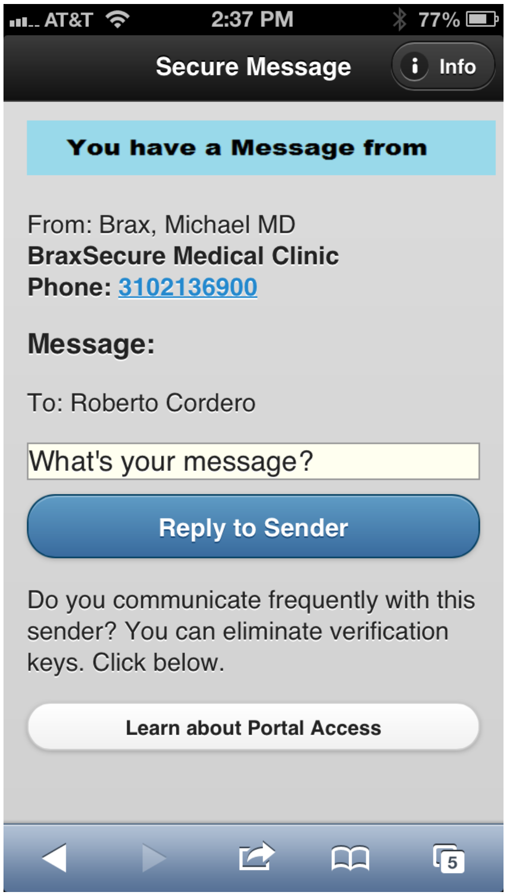
Verification Key (ID ...ace) requested.

Your Key is: demo

Please go to original message to enter key

Having the user retrieve the Verification Key via text is the most secure way of sending a message.

After entering the Verification Key, the user will be able to see the message and attachments as shown below. The message box will expand to display the message in its entirety.



You have a Message from

From: Brax, Michael MD
BraxSecure Medical Clinic
Phone: 3102136900

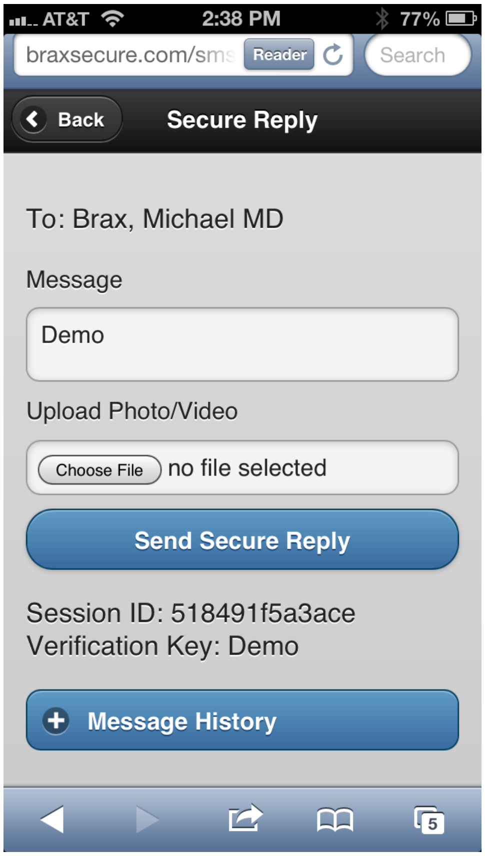
Message:

To: Roberto Cordero

What's your message?

Do you communicate frequently with this sender? You can eliminate verification keys. Click below.

From this screen, the user has the choice to Reply to Sender or activate the Patient Portal. The Reply page is shown below. As you can see, there is an option to also include an attachment. The only attachment allowed on most smartphones is a photo and video. Due to size and performance limits, we do not have the video upload enabled since there is a 10MB attachment size limit.



To: Brax, Michael MD

Message

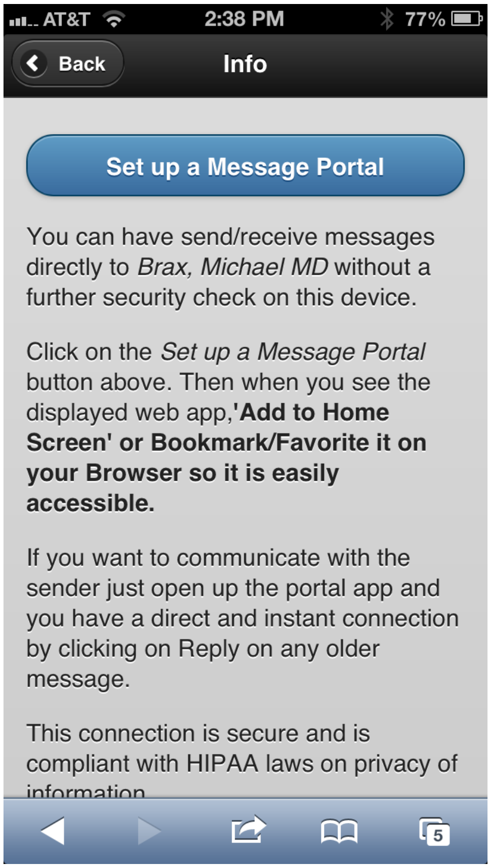
Demo

no file selected

Session ID: 518491f5a3ace
Verification Key: Demo

Notice too that the user has an option to view the Message History Thread and can then look at prior discussions with the sender.

To avoid having to constantly supply a verification key to a frequent correspondent/message sender, the app provides a "Message Portal App". To activate it, the user would click on the "Learn about Portal Access" and that will display the page below.



You can have send/receive messages directly to *Brax, Michael MD* without a further security check on this device.

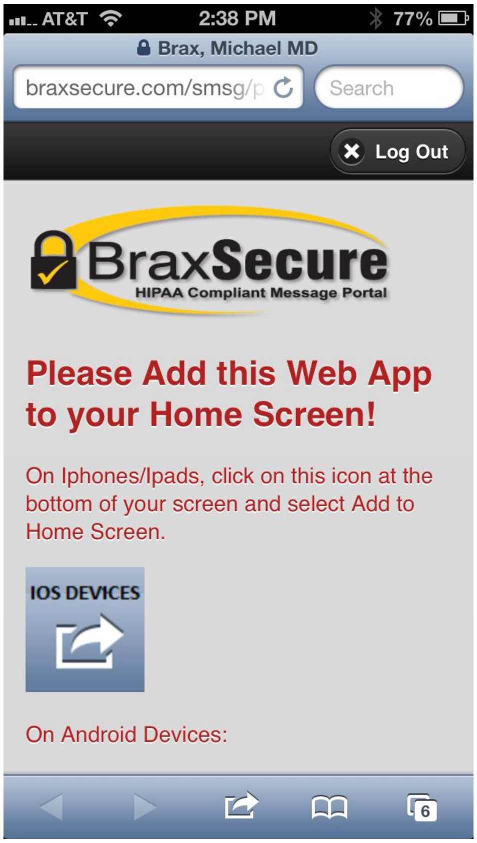
Click on the *Set up a Message Portal* button above. Then when you see the displayed web app,**'Add to Home Screen' or Bookmark/Favorite it on your Browser so it is easily accessible.**

If you want to communicate with the sender just open up the portal app and you have a direct and instant connection by clicking on Reply on any older message.

This connection is secure and is compliant with HIPAA laws on privacy of information

From this page, tapping on “Set up a Message Portal” will launch the mobile web app as shown on the next picture. The user will be asked to add the app to their home screen. What is this Message Portal? If you are a frequent communicator with a particular recipient, then it may make more sense to avoid having to supply a verification key over and over. But setting up a portal (which is a Mobile App on your Phone), the Login ID is embedded in the installation of the App. No actual passwords are kept on the device but validation is passed indirectly through a Hashed ID that is checked against the BraxSecure Server. The Hash ID is only created when you “Set Up” a portal. Each time you open a Portal from the message, it will invalidate prior occurrences of the Mobile Portal App for the recipient.

Also note that you must set up the App in the Home Screen within 30 Minutes or the Hash will be invalidated again. You will have to repeat the process of Setting Up a Portal if this happens.

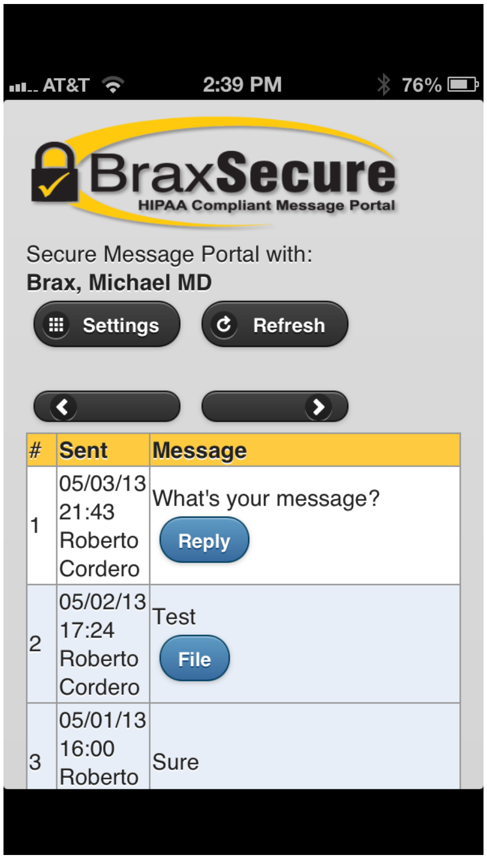


Please Add this Web App to your Home Screen!

On Iphones/Ipads, click on this icon at the bottom of your screen and select Add to Home Screen.

On Android Devices:

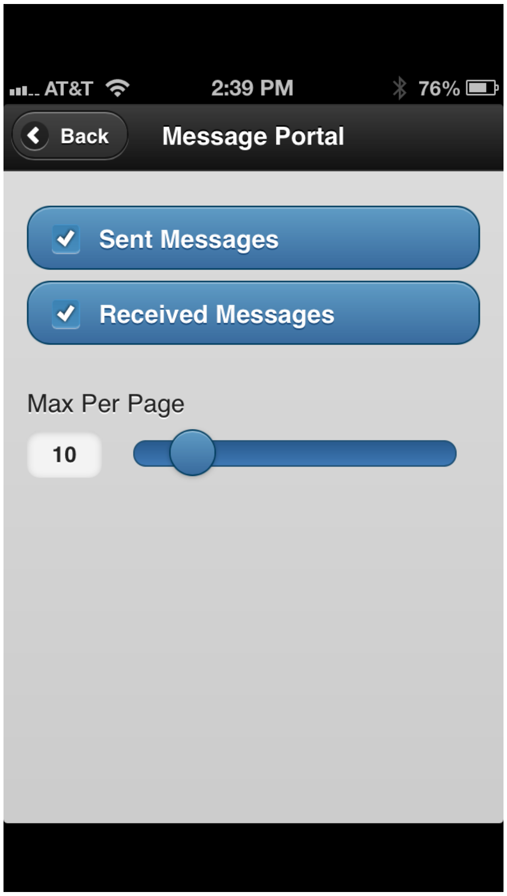
After being added to the home screen, the user can simply click on the Icon and the page below will be displayed without further login. This shows all the conversations with the sender that are still in the database (conversation that has not expired). The user can page through an unlimited number of messages.



Secure Message Portal with:
Brax, Michael MD

#	Sent	Message
1	05/03/13 21:43 Roberto Cordero	What's your message? Reply
2	05/02/13 17:24 Roberto Cordero	Test File
3	05/01/13 16:00 Roberto	Sure

Messages can be filtered based on Sent vs. Received and a maximum displayed per screen. The user can initiate a message by clicking on reply on any prior message. Also attachments are easily viewed by clicking on the File button. Note that you have to conscious of the attachments sent to each device as not all types of files can be viewed on a Mobile Device. In general, most support PDF and common image formats.



Message Portal

☑ Sent Messages

☑ Received Messages

Max Per Page

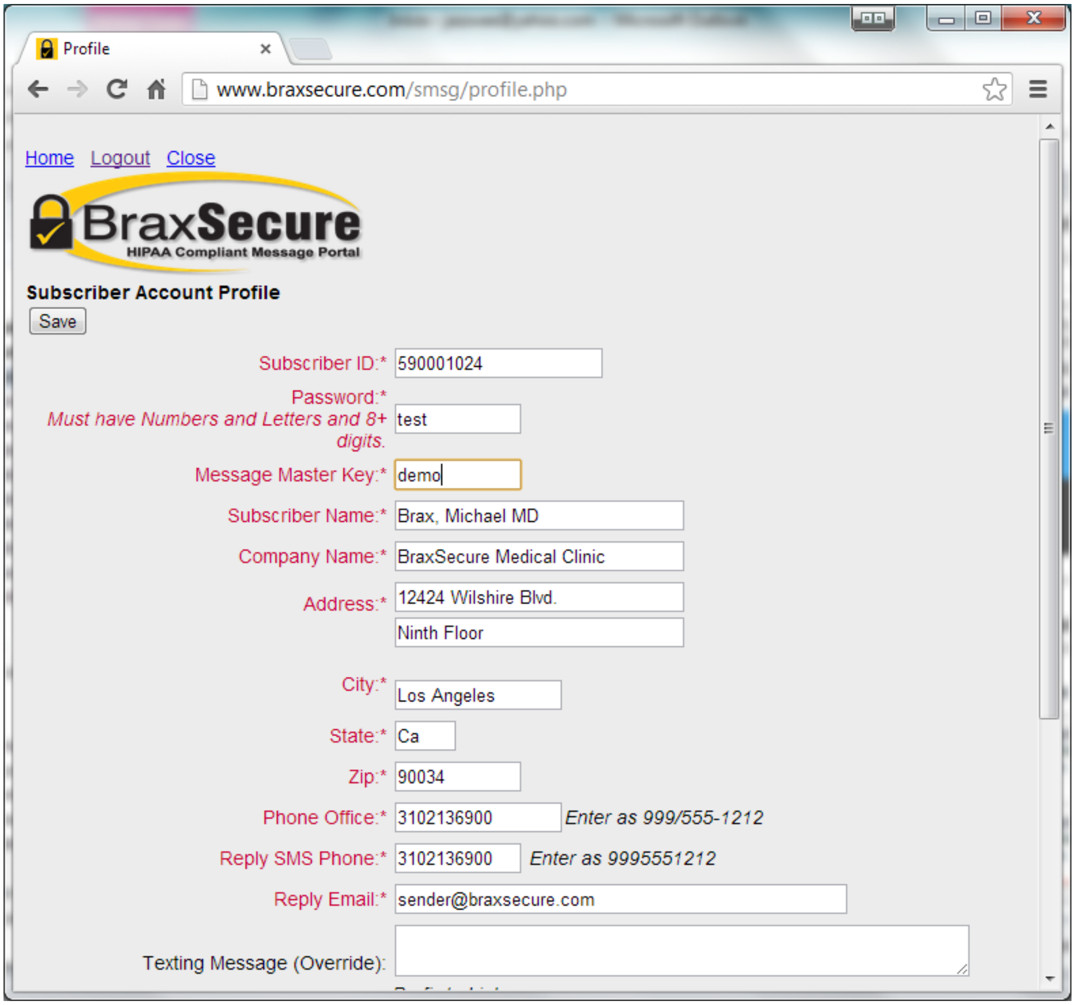
10

E. Administrative Tools

Additional tools to manage messages are provided in the Web App Desktop Version.

1. Profile

The Profile page allows a user with administrator rights to alter the account settings for the subscriber. The profile setup page is shown below.



Profile
www.braxsecure.com/smsg/profile.php
Home Logout Close
BraxSecure
HIPAA Compliant Message Portal

Subscriber Account Profile

Subscriber ID:*	590001024	
Password:* *Must have Numbers and Letters and 8+ digits.*	test	
Message Master Key:*	demo	
Subscriber Name:*	Brax, Michael MD	
Company Name:*	BraxSecure Medical Clinic	
Address:*	12424 Wilshire Blvd. Ninth Floor	
City:*	Los Angeles	
State:*	Ca	
Zip:*	90034	
Phone Office:*	3102136900	*Enter as 999/555-1212*
Reply SMS Phone:*	3102136900	*Enter as 9995551212*
Reply Email:*	sender@braxsecure.com	
Texting Message (Override):		

Important fields:

a. Password – Must have 8 characters and be a combination of numbers and letters

b. Message Master Key – this is the “shared” password for all staff users and will open any message, including one to the recipient. It is used to manage messages in the Message Manager page. This should be different from the Login ID passwords (which identify each user) and can only be used in the App only after Logging in. Note that all activities are logged by Login ID.

c. Subscriber Name – a subscriber is a single Mailbox. Therefore it cannot be a combination of several physicians as that would constitute a possible HIPAA violation. In a hospital setting, the Subscriber Name can identify a Nurse Station/Pod.

d. Address/City/State/Zip – Address of Subscriber.

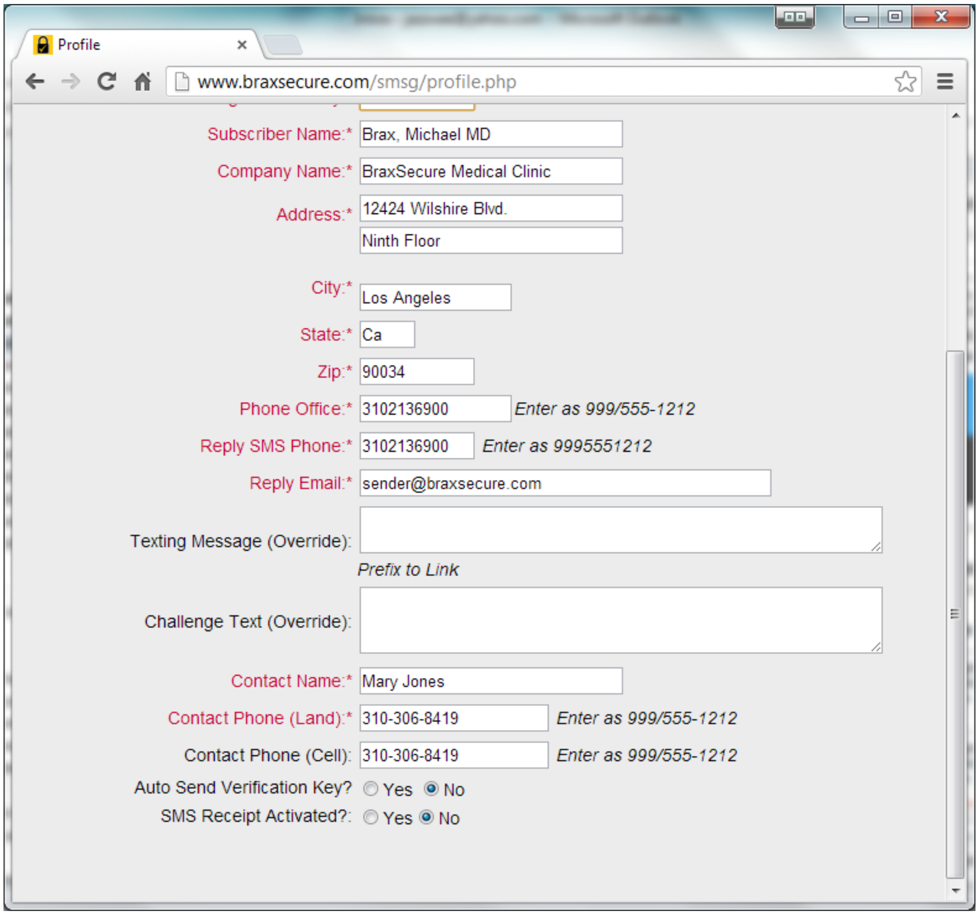
e. Phone Office – Voice Line

f. Reply SMS Phone – this is required and should be the Doctor's SMS Phone Number. Note that this is not visible to the recipient although replies will go here directly unless the Texting of Replies is suspended (feature available in Message Manager – Desktop App).

g. Reply Email – this is required and can be the common email address used for receiving email messages in the office. It NEED NOT be the Physician's primary email address since this will typically be managed by staff. So typically it will not be the address used for personal mail for the Physician.

h. Text Message (Override) – This is where one can supply an alternate message to the short message received in the text by the recipient as shown in section D above. Note that this message will Pre-pend the URL for the actual message. Be conscious of the 144 character limit for Text. The default message is:

   SubscriberName Secure Message *URL*



Subscriber Name:*	Brax, Michael MD	
Company Name:*	BraxSecure Medical Clinic	
Address:*	12424 Wilshire Blvd. Ninth Floor	
City:*	Los Angeles	
State:*	Ca	
Zip:*	90034	
Phone Office:*	3102136900	*Enter as 999/555-1212*
Reply SMS Phone:*	3102136900	*Enter as 9995551212*
Reply Email:*	sender@braxsecure.com	
Texting Message (Override):	*Prefix to Link*	
Challenge Text (Override):		
Contact Name:*	Mary Jones	
Contact Phone (Land):*	310-306-8419	*Enter as 999/555-1212*
Contact Phone (Cell):	310-306-8419	*Enter as 999/555-1212*
Auto Send Verification Key?	○ Yes ● No	
SMS Receipt Activated?:	○ Yes ● No	

i. Challenge Text (Override) – normally the challenge text is varied by Recipient. If you want to default the Challenge Text Message to something frequently used (to avoid retyping) enter it here. Sample Message:
"Enter Your NPI Number"

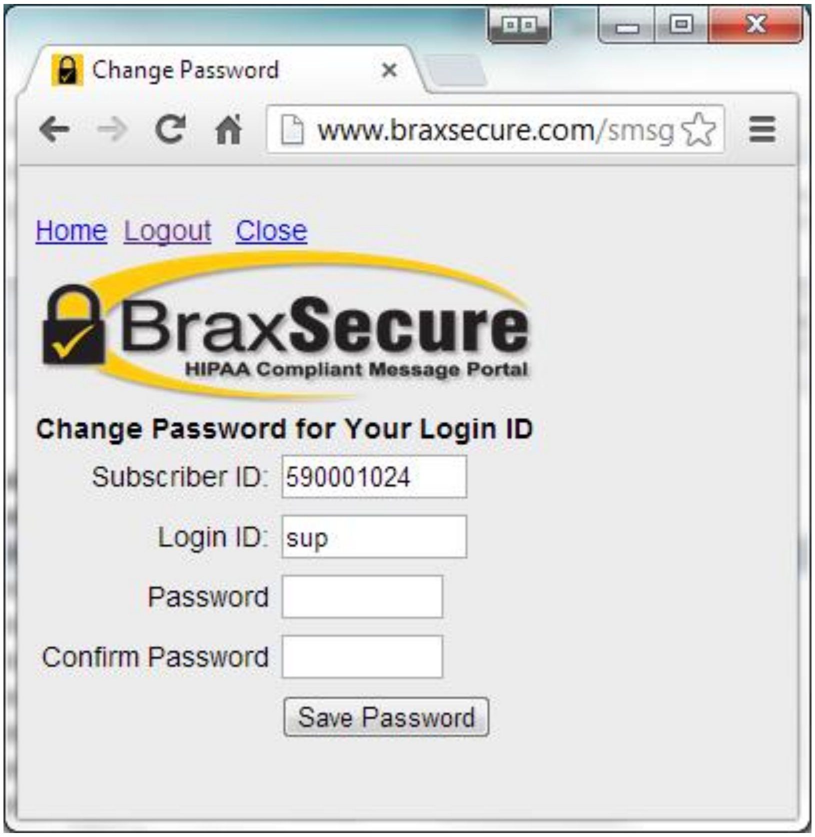
j. Contact Name/Phone Land Line/Cell Phone – Office Contact for Subscriber. Either the doctor or administrator typically.

k. Auto Send Verification Key – Not used at this time

l. SMS receipt Activated – If turned on each time a recipient reads a message, a Text Message will be sent to the SMS Sender account phone.

2. Change Password Utility

Each Logged in User can change their password at any time. The Desktop and Mobile App versions of the page are shown below. The Desktop Version obscures the Password so it is not visible to others and a confirming entry is required. This is not required in the Mobile App version since accuracy of entry is more important on the mobile device.



Change Password for Your Login ID

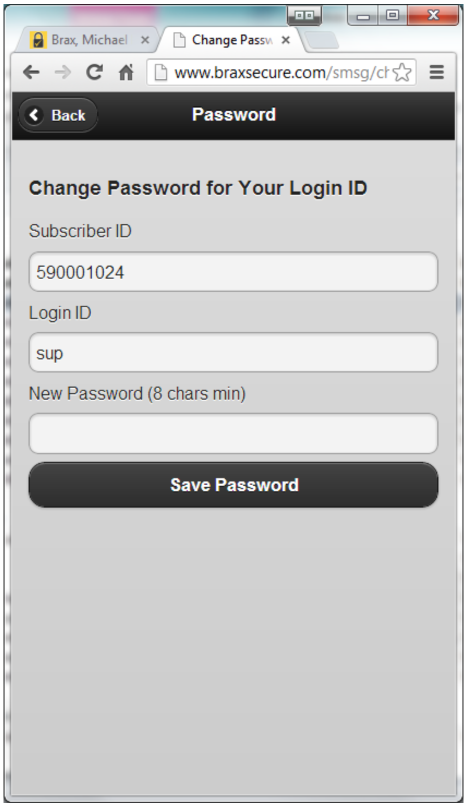
Subscriber ID: 590001024

Login ID: sup

Password

Confirm Password

The Mobile App version of Change Password looks like the page below.



Change Password for Your Login ID

Subscriber ID

590001024

Login ID

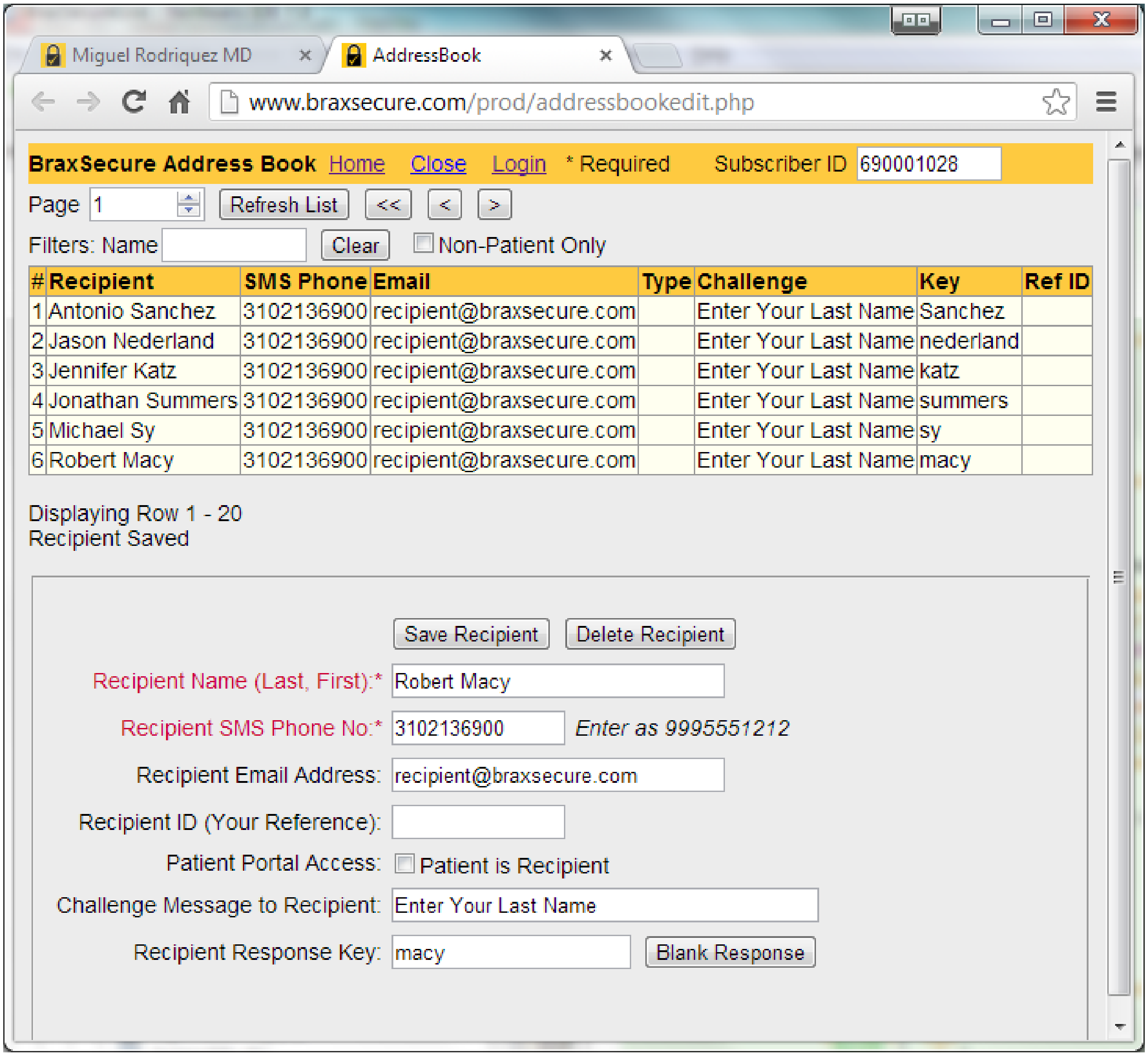
sup

New Password (8 chars min)

3. Address Book

In order to save data entry time when sending messages, recipient names, their SMS phone, and email addresses can be entered in advance. For example, if the Sender sends messages frequently to a small group of referring providers, they can be preentered here.

Also to save time, the Challenge Text and Key can be predetermined and pre-entered here. For those needing a reference number for some other system (for interface reasons), a Reference ID (like Referral ID or Patient ID) can be supplied as well. This is optional. For the purposes of identification, the system considers each name + SMS Phone number, or each email address to be a unique entity.



BraxSecure Address Book Home Close Login * Required Subscriber ID 690001028

Page 1 Refresh List << < >

Filters: Name Clear □ Non-Patient Only

#	Recipient	SMS Phone	Email	Type	Challenge	Key	Ref ID
1	Antonio Sanchez	3102136900	recipient@braxsecure.com		Enter Your Last Name	Sanchez	
2	Jason Nederland	3102136900	recipient@braxsecure.com		Enter Your Last Name	nederland	
3	Jennifer Katz	3102136900	recipient@braxsecure.com		Enter Your Last Name	katz	
4	Jonathan Summers	3102136900	recipient@braxsecure.com		Enter Your Last Name	summers	
5	Michael Sy	3102136900	recipient@braxsecure.com		Enter Your Last Name	sy	
6	Robert Macy	3102136900	recipient@braxsecure.com		Enter Your Last Name	macy	

Displaying Row 1 - 20
Recipient Saved

Save Recipient Delete Recipient

Recipient Name (Last, First):* Robert Macy

Recipient SMS Phone No:* 3102136900 *Enter as 9995551212*

Recipient Email Address: recipient@braxsecure.com

Recipient ID (Your Reference):

Patient Portal Access: □ Patient is Recipient

Challenge Message to Recipient: Enter Your Last Name

Recipient Response Key: macy Blank Response

F. Downloading the Message History

Messages are encrypted at the Server side. This means that BraxSecure administrators cannot read the messages. The only provided way to retrieve messages that have been previously downloaded is to extract them via the Download History in XML button which appears at the bottom of the Message Manager (Desktop Web App) for Administrators. If you click this, the App will export all messages currently in the system for the current Subscriber. It will show up in your download folder with the starting name of History.XML.

This data can be imported into an EHR system at some later time.

G. Message Handling Policies

1. For security reasons, messages will be kept only for 7 days by default. If your site requires a longer retention of messages, consider downloading the messages in XML as discussed above. Otherwise, please consult the Sales department to determine the small surcharge that may apply to keep messages for longer periods.

2. Message Attachments are limited to 10MB in size. Attachments are subject also to the 7 day lifespan by default. Since message attachments require large amounts of server space, a separate server may need to be set up to handle permanent storage for Patient Portal use. This is a separate charge and tied to the future Patient Portal product. A significant surcharge is applicable to retaining attachments due to the possible need to allocate a separate server.

3. Please note that you cannot call BraxSecure to have us read messages since we are unable to read the messages without your login information.